DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1.   A request for continued examination under 37 CFR 1.114, including the fee set forth in

37 CFR 1.17(e), was filed in this application after final rejection. Since this application is

eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e)

has been timely paid, the finality of the previous Office action has been withdrawn pursuant to

37 CFR 1.114. Applicant's submission filed on 09/29/2009 has been entered.

Information Disclosure Statement

2.   The following is an examiner's comment: the IDSs filed on 09/29/2009 have been

considered and Claims 1-28 and 33-35 remain allowable over the prior art of record for the

reasons noted in the Examiner's Amendment mailed on 09/04/08.

Status of Claims

3.   Claims 28-32 have been cancelled. Claim 35 has been added. Claims 1-28 and 33-35 are

pending and have been considered below.

Response to Arguments

4.   Applicant's arguments pages 13-22, filed 04/15/2009 with respect to the prior art

rejection of the claims have been fully considered and they are persuasive.

EXAMINER'S AMENDMENT

5.   An examiner's amendment to the record appears below. Should the changes and/or

additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR

1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the

payment of the issue fee.

     Authorization for this examiner's amendment was given in a telephone interview with

Mark E. Olds Reg. No. 46,507 on 06/18/2009.

     The application has been amended as follows:

     Amend the following paragraph of claim 13:

        receiving a first transport frame <u>at a communication device within the

communication network</u>, said first transport frame comprising a first encrypted data payload, a

first portion of a first sequential code, and a second portion of said first sequential code;

     Amend the following paragraph of claim 17:

        (Currently Amended) A computer-readable <u>storage</u> medium embodying

computer codes for implementing a method for synchronizing encryption and decryption of a

data frame in a communication network, the method comprising:

     Amend the following paragraph of claim 21:

        ~~means for~~ wherein said first portion of said first sequential code and said first portion of

said second sequential code identify the same relative portions of said first and second sequential

codes, and said second portion of said second sequential code represents a successive relative

portion with respect to said second portion of said first sequential code.

Amend the following paragraph of the specification:

[0084] The administration server 248 makes all administrative functions available to a

generic web browser via a HTTP web server interface with one or more pages formatted using an

Internet readable programming language ~~medium~~, such as Hyper Text Markup Language

(HTML) syntax. At least one of the administrative pages may include a reference to an

embedded Java.TM. applet. Some administrative functions may optionally be performed through

HTTP GET and POST commands issued by the web browser using conventional HTACCESS

authorization mechanisms. The administrative functions supported are generally a subset of those

supported by the CLI interface.

Allowance

6.   Claims 1-28 and 33-35 are allowed.

Examiner's Statement of Reason for allowance

7.   The following is an examiner's statement of reasons for allowance:

Barnett (US 6,661,896) is directed to a computer network security system and method.

Barnett teaches applying a key generation algorithm to a predetermined character string

at a workstation Io generate a unique encryption key and a transport key. A data packet is

encrypted based on the unique encryption key. The encrypted data packet, along with the

transport key is sent to a server. Barnett fails to disclose that the characteristic string is included in the data packet transmission.

Alden et al (US 6,101,543) is directed to a pseudo network adapter for frame capture, encapsulation and encryption. A message from the tunnel client addressed to a node reachable through the virtual private network will be passed b\' the TCP/IP slack to the pseudo network adapter 259. The pseudo network adapter 259 then encrypts the message, and encapsulates the message into a tunnel data frame. The pseudo network adapter 259 then passes the tunnel data frame back to the TCP/IP protocol slack 260 Io be sent through to the physical network adapter in the tunnel server. The tunnel server passes the received data frame to the pseudo network adapter in the server, which de-encapsulates and decrypts the message.

Citta et al (US 4,771,458) is directed to a secure data packet transmission system and method. Citta et al teaches the transmission of a global bit packet encrypted with a global encryption key followed sequentially by individually addressed packets.

Kluttz et al (6,598,161) discloses methods, systems and computer program products for multi-level encryption, wherein different encryption keys are used to encrypt different data packets (documents). See abstract. According to Kluttz et al, the document is sequentially encrypted utilizing at least two encryption keys (abstract). As shown in figure 2, there is provided a set of encryption keys (72) from which a plurality of keys (104, 106, 108) are drawn in order to encrypt the document.

Perlman (6,363,480) discloses a system and method for a user to encrypt data in a way that ensures the data cannot be decrypted after a finite period. A number of ephemeral

encryption keys are established by a first party, each of which will be destroyed at an associated time in the future (the "expiration time"). A second party selects or requests one of the ephemeral encryption keys for encrypting a message. The first party provides an ephemeral encryption key to the second party. Subsequently, the first party decrypts at least a portion of the message, using an ephemeral decryption key associated with the ephemeral encryption key provided to the second party. At the expiration time, the first party destroys all copies of at least the ephemeral decryption key, thus rendering any messages encrypted using the ephemeral encryption key permanently undecipherable.

8.   The prior art of record taken alone or in combination do not teach or render obvious the limitations as recited in independent claim 1. The cited references, whether alone or in combination fail to disclose or suggest the following limitation : "*encrypting a first data frame based on a first unique code in a first communication device, said first unique code being derived from a first sequential code; encapsulating said first encrypted data frame in a first transport frame, said first transport frame comprising a first portion and a second portion of said first sequential code; encrypting a second data frame based on a second unique code in the first communication device, said second unique code being derived from a second sequential code; encapsulating said second encrypted data frame in a second transport frame, said second transport frame comprising a first portion and a second portion of said second sequential code; and transmitting said first transport frame and said second transport frame to a second communication device, wherein said first portion of said first sequential code and said first portion of said second sequential code identify the same relative portions of said first and second*

sequential codes, and said second portion of said second sequential code represents a successive

relative portion with respect to said second portion of said first sequential code." The other

independent claims 4, 7, 10, 13, 17, 21 and 25 recite similar limitations. Consequently Claims 1-

28 and 33-35 are allowable over the prior art of record.

Any comments considered necessary by applicant must be submitted no later than the payment

of the issue fee and, to avoid processing delays, should preferably accompany the issue fee.

Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance.

Conclusion

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to FATOUMATA TRAORE whose telephone number is (571)270-

1685. The examiner can normally be reached on Monday- Friday (every other Friday off) EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Nasser Moazzami can be reached on 571 272 4195. The fax phone number for the

organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would

like assistance from a USPTO Customer Service Representative or access to the automated

information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Friday October 23, 2009.

/F. T./

Examiner, Art Unit 2436

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2436